

NETWORK SYSTEM

Publication number: JP9214493 (A)

Publication date: 1997-08-15

Inventor(s): TERADA MASATOSHI; YOSHIDA KENICHI; KAYASHIMA MAKOTO *

Applicant(s): HITACHI LTD *

Classification:

- International: G06F1/00; G06F11/30; G06F13/00; G06F15/00; G06F21/00; G06F21/20; H04L29/06; (IPC1-7): G06F11/30; G06F13/00; G06F15/00; H04L12/24; H04L12/26; H04L12/56

- European: G06F21/00; H04L12/24; H04L12/26; H04L12/56

Application number: JP19960022781 19960208

Priority number(s): JP19960022781 19960208

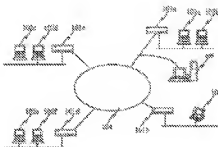
Also published as:

US5931946 (A)

Abstract of JP 9214493 (A)

PROBLEM TO BE SOLVED: To provide a computer inspection system suitable for a large scale network.

SOLUTION: A management equipment 103 distributes an external inspection program and an internal inspection program to routers 101 (101a-101d). The router 101 distributes the internal inspection program to computers 102 (102a-102f). When the inspection result of each computer 102 and obtained by executing the external inspection program and the result of the internal inspection according to the internal inspection program reported from each communication 102 indicate a fault, the router 101 commands collection of traffic log with respect to the computer 102 having the fault to a log collection device 105 and stops relay of a packet to the faulty computer 102.



Data supplied from the espacenet database — Worldwide

特開平9-214493

(43)公開日 平成9年(1997)8月15日

(51)Int.Cl. ⁶	識別記号	序内整理番号	F i	技術表示箇所
H 0 4 L 12/24		9466-5K	H 0 4 L 11/08	
12/26			G 0 6 F 11/30	E
G 0 6 F 11/30			13/00	3 5 1 H
13/00	3 5 1			3 5 3 U
	3 5 3		15/00	3 2 0 K

審査請求 未請求 請求項の数7 O L (全 12 頁) 最終頁に続く

(21)出願番号 特願平5-22761

(22)出願日 平成8年(1996)2月8日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者

寺田 真敏

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者

吉田 健一

埼玉県比企郡鳩山町赤沼2520番地 株式会社日立製作所基礎研究所内

(72)発明者

倉島 樹

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74)代理人

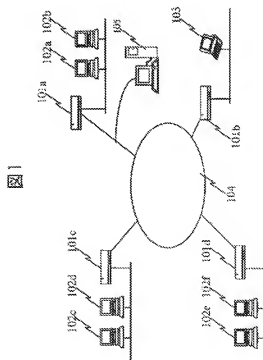
弁理士 富田 和子

(54)【発明の名称】 ネットワークシステム

(57)【要約】

【課題】大規模ネットワークに好適な計算機の監査システムを提供する。

【解決手段】管理装置103は各ルータ101に外部監査プログラムと内部監査プログラムを配布する。ルータ101は各計算機102に内部監査プログラムを配布する。ルータ101は外部監査プログラムを実行して得た各計算機102の監査結果と計算機102から報告された外部監査プログラムに従った内部監査結果に異常がある場合には、ログ収集装置105に、異常があった計算機102に関するトラフィックログの収集を指示する。また、異常があった計算機102へのパケットの中継を停止する。



【特許請求の範囲】

【請求項1】 ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、

前記ネットワークに接続した管理装置を備え、

前記管理装置は、各中継装置に、当該中継装置が他の中継装置を介さずに接続している計算機の稼働環境を前記中継装置が監査する外部監査処理の処理手順を規定する外部監査プログラムを前記ネットワークを介して配布する手段を有し、

前記中継装置は、前記管理装置から配布された外部監査プログラムに従って、前記外部監査処理を実行する手段を有することを特徴とするネットワークシステム。

【請求項2】 請求項1記載のネットワークシステムであって、

前記管理装置は、各計算機に、計算機の稼働環境を当該計算機が自身で監査する内部監査処理の処理手順を規定する内部監査プログラムを前記ネットワークを介して配布する手段を有し、

前記計算機は、前記管理装置から配布された外部監査プログラムに従って、前記内部監査処理を実行する手段を有することを特徴とするネットワークシステム。

【請求項3】 請求項2記載のネットワークシステムであって、

前記計算機は、前記内部監査処理の処理結果を、当該計算機が他の中継装置を介さずに接続している前記中継装置に報告する手段を有することを特徴とするネットワークシステム。

【請求項4】 ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、

前記中継装置は、当該中継装置が他の中継装置を介さずに接続している計算機の稼働環境を監査する手段と、監査の結果、計算機の稼働環境が正規の環境と整合しない場合に、当該計算機への前記通信の中継を抑制する手段とを有することを特徴とするネットワークシステム。

【請求項5】 ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、

ネットワークに接続し、ネットワーク上の通信の履歴を収集するログ収集装置を備え、

前記中継装置は、計算機の稼働環境を監査する手段と、監査の結果、計算機の稼働環境が正規の環境と整合しない場合に、稼働環境が正規の環境と整合しない計算機への通信の履歴の収集を、前記ネットワークを開始前記ログ収集装置に指示する手段を有し、

前記ログ収集装置は、前記中継装置より指示に応じて、指示された計算機への通信の履歴を収集することを特徴とするネットワークシステム。

【請求項6】 請求項5記載のネットワークシステムであ

って、
前記ログ収集装置には、ネットワーク上の通信の宛先として用いられるアドレスが与えられておらず、

前記ログ収集装置は、前記ネットワークの当該ログ収集装置の接続地点を通る全ての通信を監視し、通信が前記中継装置より指示である場合に、当該通信を受信することを特徴とするネットワークシステム。

【請求項7】 ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、

前記中継装置は、計算機の稼働環境を監査する手段と、監査の結果、計算機の稼働環境が正規の環境と整合しない場合に、その旨を報知する手段を有することを特徴とするネットワークシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークに接続した計算機のセキュリティに関する技術に關し、特に計算機の稼働環境の監査や、監査結果に基づく不正な侵入者に対する防御の技術に関するものである。

【0002】

【従来の技術】従来、ネットワークに接続した計算機の稼働環境の不整合を監査するシステムとしては、計算機内部から監査を実施し、計算機自身の稼働環境の不整合を計算機内部で検出する技術や、ネットワーク経由で所定の管理装置から計算機に稼働環境を問い合わせるパケットもしくはメッセージを送り、これに対する計算機の応答に基づいて管理装置において計算機の稼働環境の不整合を検出するシステムが知られている。

【0003】ここで、計算機の稼働環境の不整合とは、本来、計算機中のファイル“a”の参照は、ユーザ“a”のみ可能であるべきものが、ユーザ“x”もファイル“a”を参照可能な状態に設定されている等の設定パラメータの不整合や、本来、計算機上のアプリケーションは、コマンド“xxx”は受け付けないにもかかわらず、コマンド“xxx”を受け付けてしまう等のアプリケーションの不整合などが挙げられる。

【0004】なお、具体的には、計算機内部から計算機を監査する技術としてCOPS(Computerized Oracle and Password System)が、計算機外部の管理装置から監査する技術としてはSATAN(Security Administrator Tool for Analyzing Networks)、ISS(Internet Security Scanner)が知られている。

【0005】

【発明が解決しようとする課題】さて、現在では、インターネットなどのグローバルネットワークの発展により、世界の各地から発信された悪意を手段の計算機でリアルタイムに入手できるようになった。しかし、その反面では、各計算機は外部からの侵入者の脅威にさらされることになった。

【0006】このような侵入者に対する防衛策として、計算機の稼働環境の不整合を監視し、これを修正しておくことは不正に計算機に侵入する足掛かりを少なくするという点で重要である。不整合な環境を保持したままの計算機が1台でもあると、これを足掛かりにして不整合な環境を保持した計算機周囲の計算機にまで不正に侵入される可能性が生じる場合もある。

【0007】したがって、監査結果に異常がある場合に効果的な対策をとることが必要となる。

【0008】また、大規模なネットワークシステムを構築する場合には、管理装置と監査対象となる計算機との間で直接通信できる構成を採用できないことがある。そして、このような場合には、管理装置からの各計算機を集中的に監査することができなくなってしまう。

【0009】そこで、本発明は、大規模なネットワークを対象とした計算機の監査システムを提供することを目的とする。また、計算機の稼働環境に不整合がある場合には、稼働環境の不整合を持つ計算機への不正な侵入を防止することを目的とする。

【0010】課題を解決するための手段 前記目的達成のために、本発明は、たとえば、ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、前記ネットワークに接続した管理装置を備え、前記管理装置は、各中継装置に、当該中継装置が他の中継装置を介さずに接続している計算機の稼働環境を前記中継装置が監査する外部監査処理の処理手順を規定する外部監査プログラムを前記ネットワークを介して配布する手段を有し、前記中継装置は、前記管理装置から配布された外部監査プログラムに従って、前記外部監査処理を実行する手段を有することを特徴とするネットワークシステムを提供する。

【0011】このようなネットワークシステムによれば、随時、管理装置から中継装置が実行する監査プログラムを最新、最良のものに更新することができる。また、各中継装置が監査処理の対象とする計算機を中継装置が直接（他の中継装置を介さずに）接続している計算機としてのため、当該中継装置と当該計算機との間で必ず、直接通信することができる。また、計算機の監査のために生じる通信のトラフィックを低減することができる。従って、大規模ネットワークに好適な監査システムを実現することができる。

【0012】また、本発明は、前記目的達成のために、たとえば、ネットワークに接続した複数の計算機と、前記計算機間の通信の中継を行う複数の中継装置とを含むネットワークシステムであって、前記中継装置は、当該中継装置が他の中継装置を介さずに接続している計算機の稼働環境を監視する手段と、監査の結果、計算機の稼働環境が正常な環境と整合しない場合に、当該計算機

への前記通信の中継を抑制する手段とを有することを特徴とするネットワークシステムを提供する。

【0013】このようなネットワークシステムによれば、計算機の稼働環境が正常な環境と整合しない計算機への通信は、当該計算機には届かない。したがって、このような計算機への不正な侵入を防止することができる。

【0014】

【発明の実施の形態】以下、本発明の一次実施形態について説明する。

【0015】図1に本実施形態に係るネットワークシステムの構成を示す。

【0016】図中、103はネットワークシステムに接続した各計算機を集中的に監査するための管理装置である。101a~101dはTCP(Transmission Control Protocol)/IP(Internet Protocol)、OSI(Open Systems Interconnection)プロトコル等の所定の通信プロトコルに従った中継処理（ルーティング）を行う中継装置である。なお、本実施形態では中継装置の一例として、ルータを用いる。102a~102fは各ユーザサイトに設置されている計算機である。105はログ収集装置であり、各計算機からの処理のログ、ネットワーク上のトラフィックのログの収集を行う。

【0017】なお、本実施形態では、各装置間のデータパケットの転送には、TCP(Transmission Control Protocol)/IP(Internet Protocol)、OSI(Open Systems Interconnection)等の転送機能を使用する。そして、各中継装置101a~101dは、データパケットの中継/廃棄を行うフィルタリング機能を備える。

【0018】次に、図2に、ルータ101、管理装置103、ユーザサイトの計算機102、ログ収集装置105のハードウェア構成図を示す。

【0019】図中、204はネットワークを構成するLAN、専用線などとの入出力を制御する回線制御部である。205はディスプレイ、キーボード206を制御する端末入出力制御部である。203はプログラムや、送受信メッセージを格納するメモリである。202はプロセッサであり装置内の各部の制御を行う。回線制御部204が収容する回線数は、装置毎に異なる。計算機102、管理装置103であれば最小1つの回線を収容すればよく、ルータ101であればパケットの中継を行う最小2つの回線を収容すればよい。また、ログ収集装置であればトラフィックのログを収集する対象とする1以上の回線を収容するようとする。

【0020】次に、図3にルータ101のソフトウェア構成図を示す。

【0021】図中、302はデータパケットの転送やフィルタリングを行うための中継制御情報の格納部（ルーティングテーブル）である。データ中継制御部303は中継制御情報に基づき、データパケットのフィルタリ

グや、目的とする計算機への転送を制御する。304はネットワークとの入出力や外部の入出力装置との入出力を制御する外部インタフェース制御部であり、回線制御部204、端末入出力制御部205に配置されている。306~307は、内部ならびに外部監査プログラム群である。308は管理装置103から配布される最新の内部監査プログラム307ならびに外部監査プログラム306の受信や、配布された内部監査プログラム307の各計算機への配布を制御する監査プログラム配布・受信部である。監査制御部309は、監査結果に応じて異常の通知などの処理を行う。プログラムスケジューラ306は、301~309のプログラム実行のスケジューリングと管理を行う。

【0022】次に、図4に、計算機102のソフトウェア構成を示す。

【0023】図中、402はデータパケットを送受信するための経路情報であるデータ送受信制御情報を格納する格納部である。403はデータ送受信制御情報に基づき、目的とする計算機との間でデータパケットの送受信を行う送受信制御部である。404は回線制御部204、端末入出力制御部205に設けられ、ネットワークとの入出力、外部の入出力装置との間の入出力を制御する外部インタフェース制御部である。406a~406bは計算機上で稼動するアプリケーションである。407は内部監査プログラム、408はルータ101または、管理装置103から配布される内部監査プログラムの受信を行う監査プログラム受信部である。プログラムスケジューラ405は、402~408のプログラム実行のスケジューリングと管理を行う。

【0024】次に、図5に、管理装置103のソフトウェア構成を示す。

【0025】図中、502はデータパケットを送受信するための経路情報であるデータ送受信制御情報を格納する格納部である。503はデータ送受信制御情報に基づき、目的とする計算機との間でデータパケットの送受信を行うデータ送受信制御部である。504は回線制御部204、端末入出力制御部205に設けられ、ネットワークとの入出力、外部の入出力装置との間の入出力を制御する外部インタフェース制御部である。506はルータならびに各計算機に配布する監査プログラム群を、監査プログラムリストによって管理する管理部である。507は各ルータに最新の監査プログラムを配布するための監査プログラム配布部507である。プログラムスケジューラ505は、402~408のプログラム実行のスケジューリングと管理を行う。

【0026】次に、図6に、ログ収集装置105のソフトウェア構成を示す。

【0027】図中、1102はデータパケットを受信するための制御情報であるデータ受信制御情報の格納部である。1103はデータ受信制御情報に基づき、データ

パケットを受信するデータ受信制御部である。1104は回線制御部204、端末入出力制御部205に設けられ、ネットワークとの入出力、外部の入出力装置との間の入出力を制御する外部インタフェース制御部である。

1106はログ情報を格納するログ情報格納部である。プログラムスケジューラ1105は、1102~1108のプログラム実行のスケジューリングと管理を行う。

【0028】なお、ログ収集装置105は、以下のような特徴を有している。

【0029】(a) 図1に示すように、ネットワークを構成するLAN、専用線などの正規の接続線から分岐した分岐線に接続され、ネットワーク上に流れるデータを集集する。これは、ログ収集装置105は、ネットワーク上に流れるデータを第三者的に取り出すことを意味する。

【0030】(b) ログ収集装置105は、TCP/IP、OSI等で使用されるネットワークアドレスを持たない、従って、管理装置103、ルータ101、計算機102から、本ログ収集装置105を明示的に宛先指定してメッセージ、データパケットを送信することはない。また、ログ収集装置105からも管理装置103、ルータ101、計算機102宛にメッセージを送信することはない。

【0031】これにより、ネットワークを介してログ収集装置105に侵入し、ログ収集装置105に格納されたログ情報の改竄や破壊を行うことは、極めて困難となる。

【0032】さて、以上のような構成において、管理装置103は、外部監査プログラムと内部監査プログラムをネットワークを介して各ルータ101に配布する。さらに、各ルータ101は、管理装置103から配布された内部監査プログラムのうち計算機上で実行されるべき内部監査プログラムを各計算機102に配布する。ここでこのように、内部監査プログラムとしては、ルータ上で実行されるものと、計算機上で実行するものがある。ルータ上で実行される内部監査プログラムは、計算機上で実行される内部監査プログラムの起端と、計算機上で実行される内部監査プログラムによる監査結果の検部を行う。

【0033】以下、この内部/外部監査プログラムの配布の手順について説明する。

【0034】図7に、内部/外部監査プログラムの配布のシーケンスを示す。

【0035】図示するように、まず、管理装置103は、監査プログラム配布部506において最新の監査プログラムの一覧を作成し(601)、これに拠り、最新の内部/外部監査プログラムを、外部インタフェース制御部504より計算機の外部より監査を実施するルータ101に配布する(602)。ルータ102では、外部インタフェース制御部304で、これを受信する。そ

して、ルータ102の監査プログラム配布・受信部308は、自身が保有する内部/外部監査プログラム306、307を管理装置103より配布された内部/外部監査プログラムに更新すると共に、ユーザサイトの各計算機に配布する内部監査プログラムの一覧を作成後(603)、各計算機に内部監査プログラムを外部インタフェース制御部304を介して配布する(604)。各計算機102では、ルータ102よりの内部監査プログラムを外部インタフェース制御部304で受信する。そして、監査プログラム受信部408は、自身が保有する内部監査プログラム407の受信した内部監査プログラムへの更新を行う(605)。これにより、管理装置より、関連するルータ、計算機への最新の内部/外部監査プログラムの配布が終了する。

【0036】なお、監査制御部309の行う処理のプログラムもが外部監査プログラムと共に管理装置103から配布し、ルータ101において逐次更新するようにしてもよい。また、内部/外部監査プログラムの配布そのものは、ファイル転送、ネットワーク管理システム、メール等のメッセージ転送機能を利用することができる。また、配布にあたって監査プログラム自身の盗聴を防ぐため共有鍵や公開鍵を用いたデータパケットの暗号化し、改竄を防ぐためプログラムに対してデジタル署名を付加し、正当な送信元と宛先計算機を特定するためユーザ名、パスワード等の認証機構を付加することにより、監査プログラムの配布においても安全性の向上を図ることができる。これらの安全性を向上させる技術は、PEM(Privacy Enhanced Mail)、PGP(Pretty Good Privacy)、SNMP2(Simple Network Management Protocol 2)等において実装されている。

【0037】さて、このようにして内部/外部監査プログラムが配布されると、ルータ101は配布された外部監査プログラムを実行することにより計算機の外部よりの監査を実行する。また、各計算機は、配布された内部監査プログラムを実行することにより内部からの監査を発行する。なお、各ルータ101には、当該ルータが外部プログラムに就いて監査を行うべき計算機102、内部監査プログラムを配布すべき計算機として、直接(他のルータを介さず)に通信を行うことのできる計算機が割り当てられる。

【0038】以下、各計算機の外部/内部よりの監査の手順について説明する。

【0039】図8に、外部よりの監査のシーケンスを示す。

【0040】図示するように、まず、プログラムスケジューラ305、監査制御部309の制御下で、外部監査プログラムの実行を開始したルータ101は、外部インタフェース制御部304を介して、外側よりの監査の対象とする計算機102上のアプリケーション406に対して監査パケット901を送信する。各計算機上のアプ

リケーション406は外部インタフェース制御部404を介して受信した監査パケットに응答して、アプリケーションプログラム自身が監査パケットに응答して行った動作結果を응答パケットとして外部インタフェース制御部404を介して、ルータ101に返送する(902、903)。監査パケットは、たとえば、アプリケーションプログラムの設定パラメータを要求するものであり、응答パケットは、アプリケーションプログラムの設定パラメータを送信するものである。

【0041】ルータ101上の外部監査プログラムは、受信した응答パケットの内容と、外部監査プログラムに含まれる稼働環境の不整合がない場合の응答パケットの内容とを比較することにより、その計算機における稼働環境の不整合の有無を判断する(903)。

【0042】このように、各ルータから各計算機の外部監査を実施することにより、何らかの都合で管理装置と監査対象となる計算機とが直接通信できない場合にも外部よりの監査を実現でき、管理装置から集中的に外部監査を実施する場合に比べ、ネットワーク全体として監査時のトラフィックを低減することができる。

【0043】次に、図9に内部からの監査のシーケンスを示す。

【0044】ルータ101において、プログラムスケジューラ305、監査制御部309の制御下で起動された内部監査プログラム307は、監査の対象とする計算機102上の内部監査プログラム407に対して監査要求指示パケット1001を送信する。すると、各計算機上のプログラムスケジューラ305は、自身が保有する内部監査プログラム407を起動し(1003)する。起動された内部監査プログラム407は、内部からの監査を実施し、その結果を監査結果パケットとしてルータ101に返送する(1002)。ルータ上の内部監査プログラム307は、受信した監査結果パケットの結果を確認することにより、その計算機における稼働環境の不整合の有無を監査する(1004)。

【0045】なお、内部/外部監査プログラムによって実現される監査の内容は、個々の計算機やネットワークが提供する機能などに応じて定めるべきものであり、多種多様な内容の監査が考えられる。

【0046】ここで、図10に、以上のような外部/内部よりの監査においてルータ101と計算機102との間でやりとりされる各パケットのフォーマットを示しておく。

【0047】図10は、パケットのフォーマットを示したものである。図示するように、これらのパケットは、3つのフィールドを含み、第1フィールドにはパケットの種類、第2フィールドには操作方法、第3フィールドには転送されるデータが格納される。

【0048】外部よりの監査の際に用いられる監査ならびに監査応答パケット901は、図10(a)に示すよ

うに、パケットの種類を示す第1フィールドには「データ801a」、操作方法を示す第2フィールドには「null802a」、転送されるデータである第3フィールドには「計算機1のアプリケーションに送付するメッセージ803a」が設定される。

【0040】また、内部よりの監査の際に用いる監査実施指示パケット1001の第1～第3フィールドには、図10(b)に示すように、「監査801b」、「指示802b」、先に計算機に配布した内部監査プログラムであって、計算機上で起動せたい内部監査プログラムの一貫である「監査プログラム指示リスト803b」が設定される。また、監査結果パケット1002の第1～第3フィールドには、図10(c)に示すように「監査801c」、「結果802c」、計算機上で実行した内部監査プログラムの結果一帯である「監査結果803c」が設定される。

【0050】このようにして、計算機の外部/内部よりの監査が終了すると、各ルータ101は、内部もしくは外部よりの監査の結果を検証し、検証結果に応じた処理を行う。

【0051】すなわち、ルータ101の監査制御部309は、図11に示すように、自身が保有する外部監査プログラム、ルータ上で実行される内部監査プログラムを順次実行し(701)、これらのプログラムの実行により得られた計算機における稼働環境の不整合(異常)の有無を確認した結果、異常がある場合には(703)、監査結果を計算機管理者ならびに、システム全体を管理する管理者に通知する(704)。通知は、管理者が使用する計算機に異常を伝えるメッセージを含むパケットを外部インタフェース制御部304を介して送信し、メッセージを受けた計算機において当該メッセージを出力することなどにより行う。また、ログ収集装置に対して、監査結果に異常のある計算機へのトラフィックログの取得の開始を指示する。ログ収集装置105のデータ受信制御部1103は、この指示に従って、以降、当該計算機宛のパケットがログ情報格納部1104に蓄積していくように外部インタフェース制御部1104を制御していく。収集されたトラフィックログは、稼働環境に不整合がある計算機へのアクセス状況の記録を残すことにより、外部からの不正アクセスの検出を行う等に使用することができ、また、このようなトラフィックログの収集には、不正なアクセスを試みる者への心理的な防犯効果も期待できる。なお、本実施形態では、トラフィックログの収集を専用のログ収集装置により実施するため、データの中継装置として動作するルータのデータ転送性能を低下させることがない。

【0052】次に、一定期間中に稼働環境に不整合がある計算機への対応がなされたことを表すメッセージを受信しなかった場合に、ルータの監査制御部309は、稼働環境に不整合がある計算機へのパケットの中継を停止

させるパケットフィルタリングを假设し、稼働環境の不整合がある計算機を隔離し、計算機セキュリティを高める動作をとる。稼働環境に不整合がある計算機へのパケットの中継の停止は、ルータ101の格納部302の中継制御情報変更することにより実施する。なお、ルータ101において、稼働環境に不整合がある計算機からのパケットの中継も停止するようにしてもよい。

【0053】ところで、稼働環境に不整合がある計算機への対応は、入手により稼働環境の不整合を排除する方法や、予め登録してある対策手順に基づき対応する方法、これまでの対策手順を学習した結果に基づき計算機自身が自己修復を実施する方法などを用いる。いずれの場合も、対策が終了したら、その旨を伝えるメッセージをルータ101に計算機より送信するようにする。

【0054】一方、管理者に異常を通知してから一定期間内に対策が実施された旨のメッセージを受信した場合には、ログ収集装置105に対して、トラフィックログの取得の停止を指示する。ログ収集装置105のデータ受信制御部1103は、この指示に従って、外部インタフェース制御部1104を制御して、トラフィックログの取得を停止する。

【0055】なお、前述したように、ログ収集装置105はネットワークアドレスを与えられていない。そこで、ルータ101からのログ収集の開始、停止の指示は、ログ収集装置105が接続している伝送路に、ログ収集の開始、停止の指示を含んだパケットを送ることにより行う。そして、ログ収集装置105の外部インタフェース制御部1104において、伝送路上のこのパケットを識別し、ネットワークアドレスによらずに、取り込むようにする。

【0056】図12に、このログ収集の開始、停止を指示に使用するパケットのフォーマットを示す。

【0057】前述したようにパケットの第1フィールドはパケットの種類、第2フィールドは操作方法、第3フィールドは転送されるデータである。

【0058】図12(a)に示すように、ルータからのログ収集装置に対してログ収集の開始を指示するパケットの、パケットの種類を示す第1フィールドには「ログ1201a」、操作方法を示す第2フィールドには「開始1202a」、転送されるデータである第3フィールドにはログ収集対象として指定する計算機のリスト1203aが設定される。また、図12(b)に示すように、停止を指示するトラフィックログ収集停止パケットは、それぞれ「ログ1201b」、「停止1202b」、ログ収集対象から外される計算機リストである「ログ停止対象計算機リスト1203b」が設定される。

【0059】ログ収集装置105は、自身が接続する伝送路上のパケットを監視し、第1フィールドにログが設定されたパケットについては、これを取り込み受信する。

【0060】なお、以上の実施形態において、ネットワークへの接続前に計算機の内部ならびに外部監査を実施し、その結果に異常がないことをルータに通知しておかない限り、本ネットワークに計算機を接続しても警告を開始することができないようルータが中継の内容を設定することもできる。また、計算機間で相互に外部監査を行うようにしてもよい。

【0061】以上、本発明の一実施形態について説明した。

【0062】本実施形態によれば、

(1) 随時、管理装置からルータ、計算機が実行する監査プログラムを最新の監査プログラムに更新できる。

【0063】(2) 内部ならびに外部監査プログラムによる計算機の稼働環境を監査を行い、監査結果に異常がある場合には、これを計算機管理者ならびにシステム全体を管理する管理者に通知するので、管理者などは、稼働環境に不整合がある計算機の早期発見と早期対策を実施することができる。

【0064】(3) 稼働環境に不整合がある計算機については、ログ収集装置においてトラフィックログの収集を行うので、アクセス状況の記録に基づいた外部からの不正アクセスの検出を行うことができる。

【0065】(4) 稼働環境に不整合が発生しているが、対策の実施されない計算機については、ルータで該当計算機宛データの中継の停止を実施することにより、当該計算機への不正な侵入を排除し、ネットワークならびに計算機セキュリティを向上させることができる。

【0066】(5) ログ収集装置は、本ログ収集装置を明示的に宛先指定してメッセージを送信することはできないという機能を持つため、ネットワークを介してログ収集装置に格納されたログ情報の改竄や破壊を防ぐことができる。

【0067】

【発明の効果】 以上のように、本発明によれば、大規模

なネットワークを対象とした計算機の監査システムを提供することができる。また、計算機の稼働環境に不整合がある場合には、稼働環境の不整合を持つ計算機への不正な侵入を防止することができる。

【図面の簡単な説明】

【図1】 ネットワークの構成を示す図である。

【図2】 ルータ、計算機、ログ収集装置、管理装置のハードウェア構成例を示すブロック図である。

【図3】 ルータのソフトウェア構成を示すブロック図である。

【図4】 計算機のソフトウェア構成を示すブロック図である。

【図5】 管理装置のソフトウェア構成を示すブロック図である。

【図6】 ログ収集装置のソフトウェア構成を示すブロック図である。

【図7】 監査プログラムの配布シーケンスを示す図である。

【図8】 外部よりの監査の動作のシーケンスを示す図である。

【図9】 内部よりの監査の動作のシーケンスを示す図である。

【図10】 監査に用いるバケットの内容を示す図である。

【図11】 ルータの行う動作を示すフローチャートである。

【図12】 ログ収集の開始/停止指示に用いるバケットの内容を示す図である。

【符号の説明】

103 管理装置

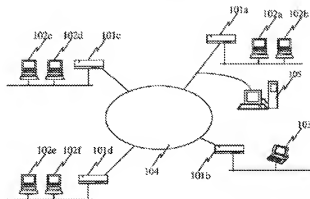
101a~101d 中継装置

102a~102f 計算機

105 ログ収集装置

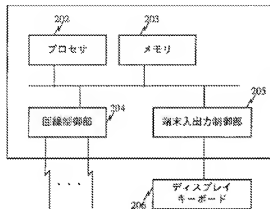
【図1】

図1



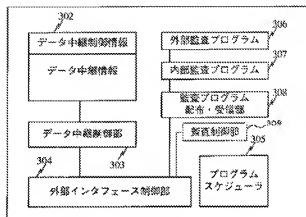
【図2】

図2



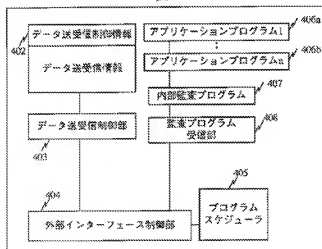
【図3】

図3



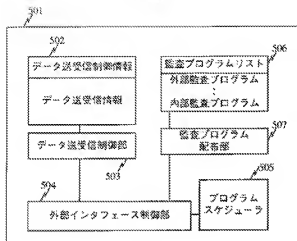
【図4】

図4



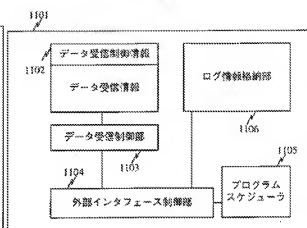
【図5】

図5



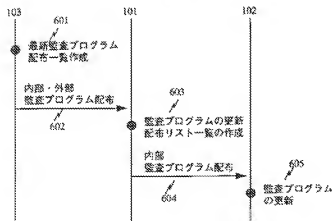
【図6】

図6



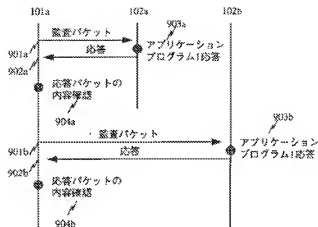
【図7】

図7



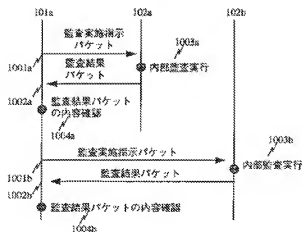
【図8】

図8



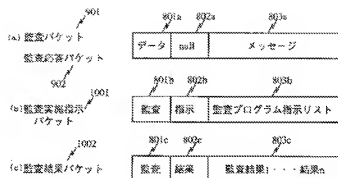
【図9】

図9



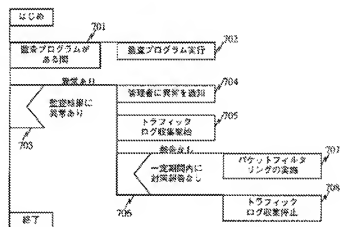
【図10】

図10



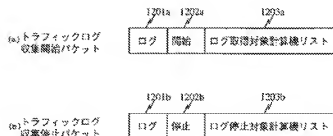
【図11】

図11



【図12】

図12



フロントページの続き

(51) Int. Cl. ⁶	識別記号	序内整理番号	FI	技術表示箇所
G 0 6 F 15/00	3 2 0		G 0 6 F 15/00	3 3 0 A
	3 3 0	9466-5 K	H 0 4 L 11/20	1 0 2 Z
H 0 4 L 12/56				